Testimony
of
Barry M. Sabin
Chief
Counterterrorism Section
Criminal Division
Department of Justice

Concerning
Information Sharing
Under Subsections 203(b) and (d) of the USA PATRIOT Act

before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
U.S. House of Representatives

April 19, 2005

Chairman Coble, Ranking Member Scott, and Members of the Subcommittee:

Introduction

Thank you for the opportunity to testify at this important hearing. Since the attacks of September 11, 2001, Congress and the Administration have made great progress in providing law enforcement and intelligence officials with the tools they need to prevent, disrupt, investigate, and prosecute terrorism. The most notable of these achievements was enactment of the USA PATRIOT Act ("Patriot Act" or "Act") in late 2001, passed with overwhelming and bipartisan support in the House and Senate.

As you know, many sections of that Act are slated to sunset later this year, unless the Congress acts to extend them. Today, I will address Section 203, and in particular, sections 203(b) and 203(d) of the Patriot Act. Both of these provisions are slated to sunset on December 31, 2005, and both deserve to be made permanent. I seek to share with you, from my perspective as a career prosecutor, how critical these provisions have been in addressing terrorist threat information, criminal investigations and the manner in which our counterterrorism mission has been performed on a daily basis.

Information-Sharing Generally

Section 203 of the Act authorizes information sharing between law enforcement and the intelligence community. As such, it complements and is complemented by other provisions of the Patriot Act that facilitate such information sharing, most notably Sections 218 and 504. These

provisions collectively have knocked down the so-called "Wall" between law enforcement and intelligence – a wall that impeded our efforts to combat international terrorism. Prior to the Patriot Act, widespread misunderstandings about the "Wall" hindered the flow of information in two directions: it hindered intelligence information from being passed to prosecutors, and it also hindered prosecutors and criminal investigators from sharing certain types of law enforcement information with the intelligence community and other national security officials. Section 203 of the USA Patriot Act was enacted to deal with the latter problem, and to ensure that valuable foreign intelligence collected by the law enforcement community can be shared with the intelligence and national security communities, under appropriate safeguards.

Mr. Chairman, you do not have to take my word on the importance of keeping that Wall down and allowing the smooth flow of terrorism-related information to appropriate agencies across the Executive Branch. The bipartisan 9-11 Commission not only called for increased information sharing within the Executive Branch, it unanimously recognized that "[t]he provisions in the [Patriot] Act that facilitate the sharing of information . . . between law enforcement and intelligence appear, on balance, to be beneficial." [1] United States Attorney Patrick Fitzgerald has given compelling testimony to Congress on the "bizarre and dangerous" complications that the "Wall" caused in major terrorism cases prior to 9/11. [2] And Director Mueller testified earlier this month that "the information-sharing provisions are consistently identified by FBI field offices as **the most important provisions in the Patriot Act**. The ability to share crucial information has significantly altered the landscape for conducting terrorism investigations, allowing for a more coordinated and effective approach" (emphasis added). [3]

Indeed, a telling example as to the importance of these information sharing provisions comes from outside the United States. A few weeks ago I met with counterterrorism officials in the law enforcement and intelligence community of one of our foreign partners. After discussing the information sharing provisions under the Patriot Act, these experienced practitioners observed that the provisions result in the following key practical consequences: (1) prosecutors are involved at the earliest stages of national security investigations; (2) the government uses a task force approach, maximizing the utility of the provisions; and (3) the provisions increase the flexibility and types of investigative techniques which can be used in a national security investigation. These developments increase the options available to decision-makers, enable them to make more informed choices and to make those choices in a more timely fashion. Hence, the legislation you have enacted in order to allow United States officials to share information is being studied by many of our partners in the international community and is paving the way for similar information sharing provisions to be incorporated into foreign laws and practices.

The Patriot Act Changes

Let me briefly review the Patriot Act changes contained in Section 203. Section 203(a) of the Patriot Act amended Rule 6(e) of the Federal Rules of Criminal Procedure to authorize the sharing of grand jury information involving foreign intelligence, counterintelligence, or foreign intelligence information, with a Federal intelligence, protective, immigration, national defense, or national security

official.

Section 203(b) of the Act authorizes law enforcement officials to share the contents of communications that were lawfully intercepted by a judicially authorized wiretap (commonly known as "Title III information") with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official, to the extent that the communications include foreign intelligence, counterintelligence, or foreign intelligence information. As with grand jury information, the disclosure can only be made to assist the recipient in the performance of his or her official duties, and the recipient may only use the information as necessary in the conduct of those duties.

Section 203(c) of the Act requires the Attorney General to establish procedures for the disclosure of the information pursuant to sections 203(a) and 203(b) when the information identifies an American citizen or other "United States person." The Attorney General has promulgated these procedures, and they require that information identifying a United States person be handled in accordance with special protocols that place significant limitations on the retention and dissemination of such information. [4]

Finally, section 203 also recognizes that criminal investigators may acquire information useful to the larger intelligence and national security communities by the use of other law enforcement techniques apart from grand juries and criminal investigative wiretaps. For example, a member of the public may walk into an FBI office and provide information on the location of an international terrorist, or the FBI may discover such information while conducting an interview or executing a search warrant. Section 203(d) of the Act authorizes the sharing of foreign intelligence, counterintelligence, or foreign intelligence information, that is obtained as part of a criminal investigation, with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official. As with grand jury and Title III information, the disclosure can only be made to assist the recipient in the performance of his or her official duties, and the recipient may only use that information as necessary in the conduct of those official duties.

Patriot Act Results and Changed Government Practices

Pursuant to the Patriot Act, intelligence emanating from criminal investigations has indeed been routinely shared, and is shared routinely, with other appropriate government officials. Some examples of intelligence information developed in a criminal case which was shared with the intelligence community under Section 203(d) include the following:

- Information about the organization of a violent jihad training camp including training in basic military skills, explosives, and weapons, as well as a plot to bomb soft targets abroad, resulted from the investigation and criminal prosecution in New York of a naturalized United States citizen who was associated with an al-Qaeda related group;

- Travel information and the manner that monies were channeled to members of a criminal conspiracy in Portland who traveled from the United States intending to fight alongside the Taliban against U.S. and allied forces;

- Information about an assassination plot, including the use of false travel documents and transporting monies to a designated state sponsor of terrorism, resulted from the investigation and prosecution in Northern Virginia of a naturalized United States citizen who had been the founder of a well-known United States organization;

- Information about the use of fraudulent travel documents by a high-ranking member of a designated foreign terrorist organization emanating from his criminal investigation and prosecution in Washington, D.C., revealed intelligence information about the manner and means of the terrorist group's logistical support network which was shared in order to assist in protecting the lives of U.S. citizens;

- The criminal prosecution of individuals from Lackawana, New York, who traveled to, and participated in, a military-style training camp abroad yielded intelligence information in a number of areas including details regarding the application forms which permitted attendance at the training camp; after being convicted, one defendant has testified in a recent separate federal criminal trial about this application practice, which assisted in the admissibility of the form and conviction of the defendants;

- The criminal prosecution in Northern Virginia of a naturalized U.S. citizen who had traveled to an Al-Qaeda training camp in Afghanistan revealed information about the group's practices, logistical support and targeting information.

Title III information is similarly being shared. The potential utility of such information to the intelligence and national security communities is obvious: suspects whose conversations are being monitored without their knowledge may reveal all sorts of information about terrorists, terrorist plots, or other activities with national security implications. Furthermore, the utility of this provision is not theoretical: the Department has made disclosures of vital information to the intelligence community and other federal officials under section 203(b) on many occasions, such as:

- Wiretap interceptions involving a scheme to defraud donors and the Internal Revenue Service and illegally transfer monies to Iraq generated not only criminal charges in Syracuse, New York but information concerning the manner and means by which monies were funneled to Iraq;

- Intercepted communications, in conjunction with a sting operation, led to criminal charges in New York and Arkansas and intelligence information relating to money laundering, receiving and attempting to transport night-vision goggles, infrared army lights and other sensitive military equipment relating to a foreign terrorist organization.

Last year, during a series of high-profile events – the G-8 Summit in Georgia, the Democratic Convention in Boston and the Republican Convention in New York, the November 2004 presidential election, and other events – a task force used the information sharing provisions under Section 203(d) as part and parcel of performing its critical duties. The 2004 Threat Task Force was a successful inter-agency effort involving robust sharing of information at all levels of government.

And the FBI relies upon section 203(d) to provide information obtained in criminal investigations to analysts in the new National Counterterrorism Center, thus assisting the Center in carrying out its vital counterterrorism missions. The National Counterterrorism Center represents a strong example of section 203 information sharing, as the Center uses information provided by law enforcement agencies to produce comprehensive terrorism analysis; to add to the list of suspected terrorists on the TIPOFF watchlist; and to distribute terrorism-related information across the federal government.

The information sharing provisions not only promote a culture of teamwork and trust they provide government officials certainty in the performance of their duties. In that regard, it should be noted that section 203 must be read in conjunction with section 905 of the Patriot Act, which generally requires that federal law enforcement agencies share foreign intelligence acquired in the course of a criminal investigation with the intelligence community, "[e]xcept as otherwise provided by law . . . ." As the Attorney General pointed out in Guidelines implementing section 905, section 203(d) makes it clear that no other federal or state law operates to prevent the sharing of such information so long as the disclosure will assist the recipients in the performance of their official duties. [5] Thus, under current law, the duty to share information under section 905 is clear. However, if section 203(d) is allowed to sunset, then each law enforcement agency's authority and duty to share foreign intelligence under section 905 may have to be reevaluated and this change might lead to unnecessary uncertainty and confusion regarding the force and effect of section 905.

These changes, and other portions of the Patriot Act, have appropriately led to changes in Department of Justice procedures and guidelines. For example, under the Attorney General's National Security Investigation Guidelines, revised on October 31, 2003, the FBI has an ongoing obligation to share investigative information from national security files with the Criminal Division and relevant United States Attorneys' Offices. In turn, the United States Attorneys and Anti-Terrorism Advisory Council Coordinators must be prepared at any time to discuss the availability of criminal charges in any international terrorism investigation within their district.

These provisions have been used repeatedly and are now a critical tool in our counterterrorism enforcement program. As Attorney General Gonzales noted in his testimony earlier this month, prosecutors in every district have worked with Joint Terrorism Task Forces over the last three years to thoughtfully and painstakingly review historical and current intelligence files to determine whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. Literally,

thousands of files were reviewed and criminal matters were pursued. The criminal cases that were filed were brought only after a full discussion as to whether criminal action was more appropriate, at that time, than continuing with covert intelligence collection. Some national security matters have continued as intelligence investigations, thereby protecting critical sources and methods. We collectively understand, and train, that the goal is prevention, not just bringing criminal prosecutions. We seek to preserve a criminal option, if it is possible, and ensure that the threat information is timely and effectively shared.

Additional Congressional Legislation

The counterterrorism community needs to pool what it knows. Indeed, that is the fundamental construct underlying many provisions of the Intelligence Reform and Terrorism Prevention Act of 2004, which was enacted by Congress just four months ago. Building upon Section 203 of the Patriot Act, provisions of the Intelligence Reform Act further expanded Federal Rule of Criminal Procedure 6(e)(3)(D) to permit an attorney for the government to disclose any grand jury matter involving international terrorism, a threat of attack or other grave hostile acts. The persons to whom this may be disclosed includes not only United States officials – including federal and state officials – but also foreign government officials "for the purpose of preventing or responding to such threat or activities." The description in the December 2004 legislation of what may be disclosed is modeled after the definition of "foreign intelligence information" used in the Patriot Act three years earlier. In light of these necessary and welcome actions by Congress in the Intelligence Reform Act, it would be incongruous to now remove the foundations from which these recent changes arise.

Similarly, after the enactment of the Patriot Act, the Homeland Security Act added two information sharing provisions to Title III. One provision (codified at 18 U.S.C. 2517(7)) authorizes the sharing of Title III information with a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the performance of official duties. Therefore, were section 203(b) allowed to expire, United States law enforcement officers would be allowed to share certain foreign information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, but would arguably not be allowed to share that same information with the CIA. And the second provision (codified at 18 U.S.C. 2517(8)) authorizes disclosure of Title III information to any appropriate federal, state, local or foreign government official to prevent or respond to a threat of attack, international terrorism, or other grave hostile acts. All of these provisions reflect Congress' continuing efforts to ensure information sharing between federal law enforcement officials and other appropriate officials.

Protecting Privacy and Civil Liberties

Section 203 fully protects legitimate privacy and civil liberties interests through its controls on disclosure and use, and its special protections for information identifying a U.S. person. For example, section 203(b) does not allow carte blanche disclosure of sensitive information. The information itself

can only be acquired in the first place pursuant to the strict demands of Title III, and section 203(b) does not in any way diminish or minimize those requirements. Second, the only information that can be shared with intelligence or national security personnel is that which satisfies the statutory definitions of "foreign intelligence," "counterintelligence," or "foreign intelligence information." [6] This requirement acts as a filter to prevent the unnecessary disclosure of extraneous information. Third, the disclosure can only be to designated federal officials, and solely for their official use. And finally, as described above, identifying information about U.S. persons is subject to special restrictions. For all these reasons, section 203(b) correctly and appropriately facilitates a unified, cohesive counterterrorism effort while also safeguarding privacy.

Section 203(d) also protects privacy. Although historically grand jury and Title III information have been treated as more sensitive than other types of law enforcement information, section 203(d) disclosure is circumscribed in much the same way as disclosure of grand jury and Title III information under sections 203(a) and 203(b). In particular, disclosure is only authorized if: (1) the information consists of foreign intelligence, counterintelligence, or foreign intelligence information; (2) the recipient is another federal law enforcement, intelligence, protective, immigration, national defense, or national security official; and (3) the disclosure is meant to assist the recipient in the performance of his or her official duties. Moreover, as with grand jury and Title III information, the recipient may only use the information as necessary in the conduct of those official duties.

Conclusion

No one should be lulled into a sense of complacency by al Qaeda's inability – so far – to mount another catastrophic attack on the U.S. homeland. Prior to 9/11, we tied ourselves in knots with misunderstood legal and bureaucratic guidelines that had the effect of constricting the flow of essential information within the United States Government. We dare not, and must not, let this happen again. Taken together, these provisions are crucial to the government's efforts to prevent and preempt terrorist attacks. We cannot put artificial barriers between law enforcement agencies and entities such as the new National Counterterrorism Center when it comes to the sharing of law enforcement information that has foreign intelligence value.

Mr. Chairman, as you debate these issues, we invite your questions, your comments, and your suggestions. We very much want to work with Congress to ensure that we will keep America safe and free. Sections 203(b) and 203(d) are helping us fight the terrorists in a manner that respects the Constitution and constitutional values. This Congress should permanently renew Sections 203(b) and 203(d) of the Patriot Act, as well as other essential provisions of the Act.

I again thank the Committee for holding this hearing. I will do my best to answer your questions.

ENDNOTES:

1. The 9/11 Commission Report, at 394 (authorized ed.).

2.See Testimony of the Honorable Patrick Fitzgerald before the Senate Judiciary Committee (Oct. 21, 2003).

3.Testimony of FBI Director Robert Mueller before the Senate Judiciary Committee (Apr. 5, 2005).

4.Memorandum of the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Identifying United States Persons (Sept. 23, 2002).

5. Memorandum of the Attorney General, Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation (Sept. 23, 2002).

6. "Foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. "Counterintelligence" means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

"Foreign intelligence information" means

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against (I) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (II) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (III) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to (I) the national defense or the security of the United States; or (II) the conduct of the foreign affairs of the United States.